REMARKS

Claims 1-50 are pending, of which Claims 1, 26, 49 and 50 are independent. All claims have been rejected under 35 U.S.C. §102. For the reasons described below, all claims are in condition for allowance.

Specification

The disclosure was objected to due to a grammatical error at page 9 of the Specification. Applicants appreciate the Examiner's careful attention to the disclosure. In response, the specification is amended. Reconsideration of the objection is respectfully requested.

Claim Amendments

Claims 1, 2, 4-14, 20, 26-37, 42, 49, and 50 are amended by the present amendment to emphasize that the software that is being identified using the claimed technique is the "protected software." In addition, Claim 1 is amended to emphasize the distinction between "supervising program" and the "protected software." Acceptance is respectfully requested.

Rejections Under 35 U.S.C. §102(b)

Claims 1-50 were rejected under §102(b) based on U.S. Patent No. 6,170,060 to Mott, et al. This rejection is traversed.

Disclosed embodiments of the present invention relate to an approach for identifying protected software using a superfingerprint. To create the superfingerprint, a supervising program selects specific portions of the protected software while the protected software is executing. The supervising program performs computations on the selected portions to obtain a collection of fingerprints. The collection of fingerprints is combined by the supervising program to create a superfingerprint of the protected software. The superfingerprint is used to identify the software.

For many purposes, including virus detection and digital rights protection, it is essential to be able to identify protected software. Conventional schemes typically rely on the filename as represented in the operating system of the computer, embedded strings in the protected software, and the size of the file on the disk to identify the protected software. However, these identification schemes do not work if the protected software has changed, either innocently or for the purposes of deception. Further, these schemes often do not work if the protected software is running from a remote computer, such as a Java applet, or if the software takes a different form when stored in the main memory of the computer and is being executed on the processor, than when it is stored on disk.

The present invention, however, provides a reliable and robust method for identifying protected software while it is being executed on the user device. First, the identifying fingerprints and superfingerprints are created according to the method set forth in Claim 1. In particular, a supervising program executes the protected software and selects portions of the executing protected software and of the results of executing the protected software, on which computations are performed. By performing computations on the selected portions, the supervising program creates fingerprints and superfingerprints. This creation of superfingerprints is set forth in Claims 1-25.

These superfingerprints are then used to identify the protected software whenever it is being executed. Namely, the superfingerprint for a protected software is stored, say on a user device. When a software application is executing, a supervising program on the device selects portions of this executing software, performs computations on those portions to produce fingerprints and compares the collection of these computed fingerprints with the stored superfingerprint for the protected software. The supervising program declares the protected software to be the same as the executing software if an approximate match is found. This method is set forth in Claims 26-50.

By way of contrast, Mott relates to a scheme to protect the transfer of protected media (such as audio files) from a library server to a client media player. Mott discusses three

authentication approaches to protect the transfer of the protected media files to the media player at the client system: (1) a point-to-point authentication protocol that verifies that the player is an authorized client and that the library server is an authorized provider; (2) a targeting protocol in which the library server assigns an identifier to the authorized player; and (3) a digital signature appended to the downloaded protected media for use by the client player to verify the media integrity and that it was originated by an authorized library server. (Mott, column 11, lines 24-48).

According to the Office Action, these digital signatures and identifiers disclosed by Mott incorporate a technology with functionality akin to the claimed superfingerprints.

However, regarding Mott's digital signatures, it is respectfully submitted that these digital signatures are not derived from executing the protected software. Rather, Mott teaches to append a digital signature to the protected media to allow the client player to authenticate the media. Specifically, Mott's approach is based on a trust architecture in which a digital signature is appended to media downloaded from the library server, and the digital signature must be authenticated by the client media player for the player to be able play the content. Mott discloses that the digital signature comprises a known bit string appended to the incoming media downloaded from library server to client computer system. Thus, similar to the prior art described at page 1, lines 14-15 of the specification, Mott's digital signatures are simply embedded strings. As such, Mott's discussion of digital signatures does not relate to the claimed fingerprints, which are derived by selecting portions of the executing protected software.

Likewise, the identifiers described in Mott are not derived from executing the protected software. In Mott, the player is assigned a unique identifier, which serves as a serial number for the player identification. Mott's player identifier is unrelated to an approach for deriving fingerprints from executing protected software.

The Examiner equates Mott's identifiers (IDs) with the claimed technique for obtaining the fingerprints by executing the protected software, and in support, the Examiner relies on the

following quote from Mott, "the private group ID is never sent through any communications link or network path, except during installation (column 12, lines 59-62). . .[t]his would be the specific execution (the installation process)." It is respectfully submitted, however, that the "installation process" described by Mott refers to the installation of the player and not to the installation of the protected media content. In fact, in Mott, the protected content is not executed unless the protected content can be authenticated using the digital signature protocol and the player has been assigned the proper identifier. Thus, Mott does not relate to the present invention that executes protected software and selects portions of the executing protected software to derive the fingerprints.

Moreover, Mott says nothing about the claimed supervising program. Mott does not discuss the claimed supervising program that performs computations on the selected portions to obtain a collection of fingerprints. Mott does not discuss the claimed supervising program that combines the collection of fingerprints to create a superfingerprint of the protected software. As such, Mott does not disclose the limitations of the claimed invention.

Therefore, it is respectfully submitted that the § 102 rejection of independent Claims 1, 26, 49 and 50 based on Mott should be withdrawn. For reasons similar to those set forth above with respect to the independent claims 1, 26, 49 and 50, the § 102 rejection of dependent claims 2-25 and 27-48 should be withdrawn. Reconsideration of the rejections under § 102 is respectfully requested.

Information Disclosure Statement

A Supplemental Information Disclosure Statement (SIDS) is being filed concurrently herewith. Entry of the SIDS is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If

the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By _____
James M. Smith
Registration No. 28,043
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133
Dated: 8/11/06